

(19)日本国特許庁 (J P)

## (12)公開特許公報 (A)

(11)特許出願公開番号

特開平5-81204

(43)公開日 平成5年 (1993) 4月2日

(51)Int. Cl.<sup>5</sup>G 0 6 F 15/00  
13/00

識別記号

3 3 0 B 8219-5L  
3 5 1 Z 7368-5B

庁内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数5 (全 5 頁)

(21)出願番号 特願平4-48618

(22)出願日 平成4年 (1992) 3月5日

(31)優先権主張番号 9 1 0 4 9 0 9 . 8

(32)優先日 1991年3月8日

(33)優先権主張国 イギリス (GB)

(71)出願人 590003191

インターナショナル コンピューターズ  
リミテッドイギリス国, ロンドン エスタブリユ15 1  
エスタブリユ ブットニー, アイシーエル  
ハウス (番地なし)

(72)発明者 トーマス アンソニー パーカー

イギリス国, エスエヌ11 9エヌエフ, ウィ  
ルトシャー, クレイン, デリー ヒル, オー  
ルド ロード 59

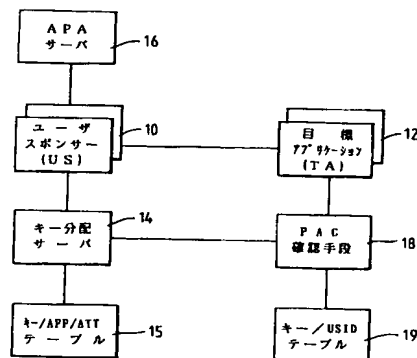
(74)代理人 弁理士 岡部 正夫 (外5名)

(54)【発明の名称】 分散型コンピュータシステムにおけるアクセス制御

(57)【要約】 (修正有)

【目的】 特権属性証明書 (PAC) の代理使用を制御すると同時にPACを多くの目標に使用できるようにする方法の提供。

【構成】 システムのユニットが他のユニットと連絡するための暗号キーを配給するキー分配サーバ14があり、これには各目標アプリケーション12をエントリするための目標アプリケーション12のマスターキー値と共にアプリケーション身元 (APP) 属性 (ATT) を含んだテーブル15が伴っている。認証及び特権属性サーバ (APAサーバ) 16はユーザを認証し、キー分配サーバ14と連絡できるようにユーザ・スポンサー10にセッションキー及びPACを配給する。また、目標アプリケーション12に提示されたPACを確認するPAC確認手段18及びキーとユーザ身元との間の関連を形成できるテーブル19を備えている。



1

## 【特許請求の範囲】

【請求項1】 複数の開始者実体(10)が複数の目標実体をアクセスできるデータ処理システムであって、前記システムが

- a) 開始者実体に特権属性証明書(PAC)を配給する手段(16)と、
- b) 前記PACを確認する確認手段(18)と、
- c) 開始者実体に暗号キーを配給するキー分配手段(14)とからなり、更に前記システムが、

(i) 各開始者実体(10)は一組の開始者資格付与属性を割り当てられ、

(ii) キー分配手段(14)によって開始者実体に配給された前記各キーは暗号的にそれと関連する開始者実体の開始者資格付与属性を有し、

(iii) 各PACは開始者実体またはPACを使用する権利を与えられた実体に相当する開始者資格付与属性を含み、

(iv) 確認手段(18)が確認のためにPACを受け取るとき、前記確認手段は、PACにおける開始者資格付与属性が前記確認手段と連絡するために使用される前記キーと関連した開始者資格付与属性に整合しているかどうかを照合することを特徴とするシステム。

【請求項2】 前記確認手段が、前記キーを前記開始者実体の身元に関連付けるテーブルを保有していることを特徴とする請求項1記載のデータ処理システム。

【請求項3】 前記開始者実体が、ユーザとシステムの間のインターフェースを供給するように特定のエンドユーザの代わりに実行するための少なくとも1つのユーザ・スポンサーを含むことを特徴とする請求項1または2記載のシステム。

【請求項4】 前記目標実体が少なくとも1つのアプリケーションプログラムを含むことを特徴とする請求項1、2又は3記載のシステム。

【請求項5】 複数の開始者実体が複数の目標実体をアクセスできるデータ処理システムの操作方法において、前記方法が

- a) 開始者実体に特権属性証明書(PAC)を配給する工程であって、前記各々のPACが、PACを使用する権利を与えられた開始者実体に相当する開始者資格付与属性を含むもの、

- b) 開始者実体に暗号キーを配給する工程であって、前記各々のキーがそれと暗号的に関連する開始者実体の開始者資格付与属性を有しているもの、及び

- c) PACにおける開始者資格付与属性がPACに連絡するために使用される前記キーと関連する開始者資格付与属性と整合している否かを照合する工程からなることを特徴とする方法。

## 【発明の詳細な説明】

【0001】

2

【産業上の利用分野】 本発明は、分散型コンピュータシステムにおける目標アプリケーションに対するユーザによるアクセスを制御するための方法及び装置に関する。

【0002】

【従来の技術】 分散型コンピュータシステムにおけるセキュリティのための構成は、欧州コンピュータ製造業者協会(ECMA)によって提案された。これは、以下の参考資料に記載されている。

- 1) ECMA TR/46 “オープンシステムにおけるセキュリティ・セキュリティ構成(Security in Open Systems - a Security Framework)” 1988年7月版
- 2) ECMAスタンダード ECMA/138 1989年12月版
- 3) “ネットワーク・アクセス・コントロール・ディベロップメント(Network Access Control Development)” COMPACS 90 カンファレンス, ロンドン, 1990年3月版

【0003】 ECMAセキュリティ構成は、ユーザがシステムに認証されることを可能にすると共にユーザがアクセス権の認証済集合に相当する特権属性証明書(PAC)と呼ばれるデータパッケージを結果として得ることを可能にする。ユーザは、目標アプリケーションをアクセスしたいとき、ユーザのアクセス権の証拠としてそのアプリケーションに対してPACを提示する。このようなPACの使用については、本願の出願人による同時出願中の英国特許出願第9015104、4号に記載されている。

【0004】 目標アプリケーションに提示されたPACを確認するために、目標アプリケーションによって使用され得るPAC確認手段(PVF)と呼ばれる特殊ユニットを提供することが提案された。

【0005】 また、システムにおける他のユニットとの連絡に使用するために、請求があり次第ユーザ及びアプリケーションに対して暗号キーを与える機能を有するキー分配サーバ(KDS)と呼ばれる特殊ユニットを提供することが提案された。

【0006】 PACは、通常、いくつかの異なる目標アプリケーションをアクセスするために、ユーザによって数回使用され得る。また、ユーザの代わりにさらに別の目標アプリケーションをアクセスするために、“代理”としてPACを使用することが目標アプリケーションに許され得る。しかし、もし最初の目標アプリケーションがPACを誤用しないと信用され得なければ、このような代理使用は望ましくない。

【0007】

【発明が解決しようとする課題】 本発明の目的は、PACの代理使用を制御すると同時にPACを多くの目標に使用できるようにする方法を提供することにある。

【0008】

【課題を解決するための手段】 本発明によれば、複数の

開始者実体(10)が複数の目標実体をアクセスできるデータ処理システムであって、前記システムが

- a) 開始者実体に特権属性証明書(PAC)を配給する手段(16)と、
- b) 前記PACを確認する確認手段(18)と、
- c) 開始者実体に暗号キーを配給するキー分配手段(14)とからなり、

更に前記システムが、(i) 各開始者実体(10)は一組の開始者資格付与属性を割り当てられ、(ii) キー分配手段(14)によって開始者実体に配給された前記各キーは暗号的にそれと関連する開始者実体の開始者資格付与属性を有し、(iii) 各PACは開始者実体またはPACを使用する権利を与えられた実体に相当する開始者資格付与属性を含み、(iv) 確認手段(18)が確認のためにPACを受け取るとき、前記確認手段は、PACにおける開始者資格付与属性が前記確認手段と連絡するために使用される前記キーと関連した開始者資格付与属性に整合しているかどうかを照合することを特徴とするシステムが提供される。

【0009】

【実施例】本発明による分配処理システムの一例を、添付図面を参照しつつ以下に説明する。

【0010】図1において、本システムは多数のユーザ・スポンサーユニット(US)10を含み、各ユニットは特定のエンドユーザの代わりをつとめる。例えば、USはユーザとシステムの残りの部分との間のインターフェースを供給するため、ユーザのワークステーションで動作するソフトウェアモジュールになり得る。

【0011】本システムは、更に、ユーザによってアクセスされ得る多数の目標アプリケーション(TA)を含む。この目標アプリケーションは、データベースソフトウェアまたは処理ソフトウェアを含み得るものである。

【0012】システムにおけるユニットに暗号キーを配給し、該ユニットを他のユニットと連絡させることができるようにするために、キー分配サーバ(KDS)が備えられている。このKDSは、各目標アプリケーションのためのエントリを保有するテーブル15を伴って備えられている。各エントリは、KDSと目標アプリケーションに分配されるマスターキー値を含んでいると共に、管理されたアプリケーション身元(APP)とアプリケーションに関連する1つ以上のアプリケーション属性(ATT)とを含んでいる。

【0013】ユーザ・スポンサーに関するステート情報は、KDSに保有されている必要はない。

【0014】ユーザを認証し、KDSと連絡できるようにユーザ・スポンサーにセッションキーを配給し、特権属性証明書(PAC)を配給するために、認証及び特権属性サーバ(APAサーバ)16が備えられている。

【0015】また、本システムは、目標アプリケーションに提示されたPACを確認する機能を有するPAC確

認手段(PVF)18を含んでいる。このPVFは、後述するように、キーとユーザ身元との間の関連を形成できるテーブル19を保有している。

【0016】以下の説明においては、次の表示法が使用される。

(XXX) K これは値XXXがキーKの下で暗号化されていることを意味する。

[XXX] K これは値XXXがキーKの下で暗号でサインされるかまたは捺印されていることを意味する。

10 【0017】暗号化または暗号でサインもしくは捺印する技術は、技術上周知なので、ここではさらに詳細に説明することを要しない。

【0018】「ユーザ・スポンサーによるPACの使用」図2a乃至2dにおいて、ユーザ・スポンサー(US)が目標アプリケーションをアクセスすることを要求するときに次の手続きが行われる。

20 【0019】図2a: USは、APAサーバに対してユーザを認証し、KDSと連絡できるセッションキーSKとユーザの代わりにPACとを供給することを要求する。APAサーバは、USに対して次の情報を返す。

(SK) CK

(USID, SK) KA

ここで、CKはユーザがシステムに初めにログオン(log on)したときにUSとAPAサーバ間に開設された連絡キーであり、KAはAPAサーバ及びKDSに対してのみ知られているマスターキーであり、USIDはAPAサーバによってUSに割り当てられた唯一の身元である。この身元USIDは任意の唯一の値でよい。どんな方法でもAPAサーバに登録されてしまうことは、US

30 【0020】また、APAサーバは、請求されたPACをAPAサーバのプライベートキーPKの下に暗号でサインしてUSに返す。APAサーバは、PACの予め決められたフィールド内に、請求しているUSの身元USIDを挿入する。もしPACの代理使用が許されるべきことであるなら、APAサーバは同様に、アプリケーション身元APP、及び/又は前記代理使用が可能な各アプリケーションの属性ATTを、PAC内に挿入する。PAC内のこれらの値(USID, APP及びATT)

40 【0021】図2b: 次にUSは、KDSと連絡するためキーSKを使用し、USとPVF間の連絡のためのベーシックキーKBを供給するようKDSに請求する。この請求は、上述のようにAPAサーバから得られた値(USID, SK) KAを含むものである。

50 【0022】KDSは、USと連絡するためのキーSKを得るために、キーKAを使用してこの値を解読する。これと同時に、KDSは、請求しているUSの身元USIDを得る。

【0023】次に、KDSはUSに次の情報を返す。

(KB) SK

(USID, KB) KS

ここで、KSはKDS及びPVFに対してのみ知られているシークレットキーである。

【0024】図2c：次にUSは、USとPVF間の連絡に使用されるべきベーシックキーKBの情報を知らせるために、PVFに情報(USID, KB) KSを送る。PVFは、KBを得るためにキーKSを使用してこれを解読する。同時に、PVFはUSの身元USIDを得て、その結果、テーブル19内に適切なエントリを作ることによって、身元USIDとキーKB間の関連を形成することができる。

【0025】図2d：USは、目標アプリケーションTAをアクセスすることを請求するとき、APAサーバから得たサイン済PACを含む情報を送る。TAは、確認のためPVFにこのPACを提示する。

【0026】PVFは、それが有効であることを保証するためにPACを照合する。また、PVFは、PACのIQAフィールド内のUSIDを、キーKBと関連するUSIDの値と比較する。もしそれらが等しくなれば、それは不正なソースによって申し込まれているものなので、PACは無効なものとして見做される。

【0027】「PACの代理使用」次に、図3a乃至3cを参照し、ユーザの代わりに第2の目標アプリケーションTA2をアクセスするため、第1の目標アプリケーションTA1が、ユーザ・スポンサーから得たPACの代理使用をすることを請求する場合について説明する。

【0028】図3a：アプリケーションTA2は、目標アプリケーションTA2と連絡できる対話キーの請求をKDSに最初にする。この請求は、KDSとアプリケーションTA1に分配されるマスターキーKKAの下で捺印される。

【0029】この請求に回答して、KDSは、キーKKAを含むエントリを見つけるためにテーブル15を調べ、そして請求しているアプリケーションに情報(KAT) KKAを返す。ここで、KATはTA1とTA2との間の連絡のために必要な対話キーである。

【0030】また、KDSはパッケージ(APP, ATT, KAT) KKTを返す。ここでAPP及びATTは、参照したテーブルエントリから得られるアプリケーション身元及び属性であり、KKTは、KDSとTA2に分配されるマスターキーである。

【0031】図3b：次に、アプリケーションTA1は、パッケージ(APP, ATT, KAT) KKTをPVFに送る。PVFはこれを解読し、それによりAPP, ATTとキーKATとの間の関連を形成し、適切なテーブルエントリを作ることができる。

【0032】図3c：TA1は、TA2をアクセスすることを請求するとき、TA2にサイン済PACを送り、

続いてTA2は確認のためPVFにこれを提示する。次に、PVFは、PACのIQAフィールド内のAPP及びATTがキーKATと関連するそれらと整合するかどうかを照合する。もし整合していれば、次にTA1によるPACの代理使用が許され、その結果PACが有効とされる。そうでなければ、PACは無効なものとして見做される。

【0033】「PVFの動作」要約すれば、PVFは確認のためPACを提示されるときに、次の条件が満足されるかどうかを照合する。

—PACにおけるUSIDが、使用されたキーとテーブル19内で関連するいずれのUSIDとも等しいこと、及び

—PACにおける開始者資格付与属性(IQA)のうちの1つが、使用されたキーと関連する属性として現れること。

【0034】もしこれらの条件のいずれもが満足されるなら、その時PACは有効とされ得る。さもなければ、PVFはPACが無効なものとして宣言する。

【0035】USはどんな方法でも認証される必要がないことに注目すべきである。証明されている事は、PACを請求された同一実体が、PVFにそれを申し込んでいるということである。

【0036】本発明の別の形式において、プロテクションの同一形式が、PACの獲得を認定するために使用された認証証明書(ECMA-138を参照、この中で認証証明書は「認証済身元」と名づけられている。)に対して可能な場合、APAサービスの認証及びPAC供給態様は、別々に実行され得る。

【0037】

【発明の効果】以上説明したように、本発明によれば、PACの代理使用を制御すると同時にPACを多くの目標に使用できるようにする方法が提供される。

【図面の簡単な説明】

【図1】本発明による処理システムのブロック図である。

【図2】aはシステムの動作を示すシーケンス図である。

bはシステムの動作を示すシーケンス図である。

cはシステムの動作を示すシーケンス図である。

dはシステムの動作を示すシーケンス図である。

【図3】aはシステムの動作を示すシーケンス図である。

bはシステムの動作を示すシーケンス図である。

cはシステムの動作を示すシーケンス図である。

【符号の説明】

10 ユーザ・スポンサーユニット(US)

12 目標アプリケーション(TA)

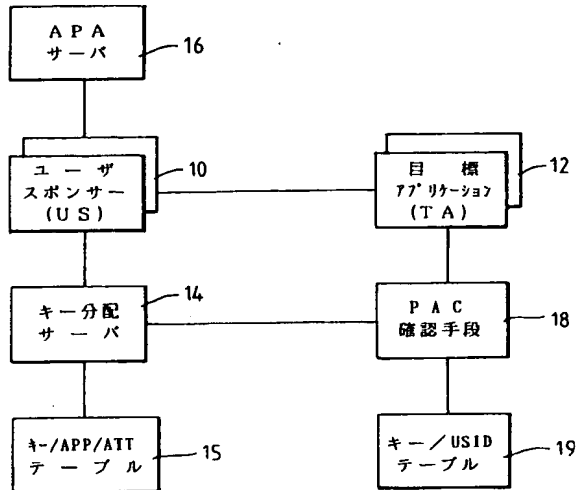
14 キー分配サーバ(KDS)

15 キー/APP/ATT・テーブル

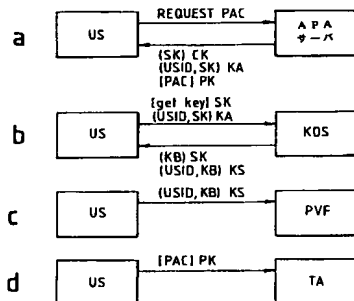
- 16 認証及び特権属性サーバ (APAサーバ)  
 18 PAC確認手段 (PVF)

- 19 キー/USID・テーブル

【図1】



【図2】



【図3】

